Available online at www.sciencedirect.com

ScienceDirect

Finite Fields and Their Applications 13 (2007) 727–737

FINITE FIELDS AND THEIR APPLICATIONS

http://www.elsevier.com/locate/ffa

Error-correcting codes on low rank surfaces

Marcos Zarzar

Department of Mathematics, University of Texas, Austin, TX 78712-0257, USA

Received 1 April 2005; revised 4 May 2007

Available online 17 May 2007

Communicated by Jacques Wolfmann

Abstract

In this paper we construct some algebraic geometric error-correcting codes on surfaces whose Néron–Severi group has low rank. If the Néron–Severi group is generated by an effective divisor, the intersection of this surface with an irreducible surface of lower degree will be an irreducible curve, and this makes possible the construction of codes with good parameters. Such surfaces are not easy to find, but we are able to find surfaces with low rank, and those will give us good codes too.

Keywords: Error-correcting codes; Algebraic geometric codes; Weil restriction of scalars; Algebraic surfaces

1. Introduction

In the eighties the Russian mathematician and engineer V.D. Goppa [4] introduced the idea of constructing error-correcting codes on algebraic curves by evaluating certain spaces of functions on points of a curve. Let $\mathbb{F}_q$ denote the finite field with q elements. Let C be an algebraic curve of genus g defined over $\mathbb{F}_q$, $D = P_1 + P_2 + \cdots + P_n$ and G divisors on C such that $\operatorname{supp}(D) \cap \operatorname{supp}(G) = \phi$. Let

$$\mathcal{L}(G) = \left\{ f \in \mathbb{F}_q(C) \;\middle|\; (f) \geqslant -G \right\} \cup \{0\}.$$

Observe that $\mathcal{L}(G)$ is a $\mathbb{F}_q$-vector space. The Geometric Goppa code associated with the divisors D and G is defined as the image of the map

E-mail address: zarzar@math.utexas.edu.

1071-5797/$ – see front matter
doi:10.1016/j.ffa.2007.05.001

$$\varphi : \mathcal{L}(G) \to {\mathbb{F}_q}^n$$
$$f \mapsto \big(f(P_1), f(P_2), \ldots, f(P_n)\big).$$

The Riemann–Roch theorem gives us a lower bound for the minimum distance, and so the parameters for this code are $k = \dim(G) - \dim(G - D)$ and $d \geqslant n - \deg(G)$. On curves, points can be thought as divisors, and the Riemann–Roch theorem makes possible a good description of these codes. The construction of Goppa works for any algebraic variety, not necessarily for curves only. Over a surface, the construction can be made in the following way:

Given a divisor G on a projective surface X, both defined over the finite field $\mathbb{F}_q$, and rational points $P_1, \ldots, P_n$ on X but not on G, we can define a code C consisting of the vectors $(f(P_1), \ldots, f(P_n))$ where f varies in $\mathcal{L}(G)$.

The construction of good codes on higher-dimensional varieties is more complicated, by the simple fact that, generally speaking, it is not easy to estimate and control the number of zeros of algebraic functions on higher-dimensional varieties. The reason for constructing codes on surfaces whose Néron–Severi group is generated by a single effective divisor is the following: if we intersect it with an irreducible surface of lower degree (both surfaces in $\mathbb{P}^3$), we obtain an irreducible curve, and this results in good parameters for the code. Unfortunately, such surfaces are not easy to find, but we are able to construct good codes using surfaces with low rank, not necessarily 1.

2. A first case

In [8], Swinnerton-Dyer lists all the possibilities for the zeta function of a non-singular cubic surface over a finite field. He shows that the zeta function depends only on the rationality properties of the 27 lines contained in the surface in the following way: the Frobenius endomorphism σ induces a permutation σ^* of the lines and σ^* is an element of G, the group of permutation of the lines which preserve incidence relations. Then for each conjugacy class in G he determines the zeta function of the surface. There are 25 conjugacy classes in total, and among those we have the possibility of having a cubic surface defined over $\mathbb{F}_q$ with $q^2 + 2q + 1$ points, and having Néron–Severi group of rank 1 [8, Class 12 of Table 1, p. 57]. Any other cubic listed in [8] with more than $q^2 + 2q + 1$ points will potentially have rank higher than 1. The existence of a cubic surface in $\mathbb{P}^3$ with $q^2 + 2q + 1$ points and Néron–Severi group of rank 1 allows the construction of a good code, as we will see. To estimate the minimal distance of this code, we need the following lemma.

Lemma 2.1. *Let $X \subset \mathbb{P}^3$ be a smooth surface of degree d defined over $\mathbb{F}_q$, with d not divisible by the characteristic of $\mathbb{F}_q$. Assume that the rank of the Néron–Severi group of X is 1 and its generator is an effective divisor. Let $Y \subset \mathbb{P}^3$ be an irreducible surface of degree $1 \leqslant m < d$ defined over $\mathbb{F}_q$. Then $X \cap Y$ is irreducible.*

Proof.

Step 1. *$Pic^o(X) = 0$ (this works for any smooth surface in $\mathbb{P}^3$).*

Proof. Mumford (in [5, theorem on p. 196]) shows that

$$\dim\big(Pic^o(X)\big) \leqslant \dim\big(H^1(X, \mathcal{O}_X)\big)$$

and since $X \subset \mathbb{P}^3$ and X is smooth, Beauville (in [2, Lemma VIII.9, p. 99]) shows that

$$\dim\big(H^1(X, \mathcal{O}_X)\big) = 0$$

and so $\dim(Pic^o(X)) = 0$.

Step 2. *Let C_0 be a plane section of X. Then $NS(X) = C_0\mathbb{Z}$.*

Proof. Here on Step 2 we will be working over an algebraic closure of $\mathbb{F}_q$. It does not affect the overall argument of the lemma. By hypothesis, $NS(X)$ is cyclic of rank 1 so if D is a generator, C_0 is algebraically equivalent to nD for some $n \in \mathbb{Z}$ with $n > 0$ (since D is effective). By Step 1 above, C_0 is linearly equivalent to nD. But D is effective, implying that nD is a plane section of X. Let $H = nD$.

Suppose that x, y, z and w are projective coordinates and, applying a change of coordinates if necessary, suppose that H is given by $w = 0$. So $X \cap H$ is given by $h(x, y, z)^n$. Let g be such that X is given by $g = 0$. Then

$$g(x, y, z, w) = h(x, y, z)^n + wR(x, y, z, w)$$

for some R, since $X \cap H$ is given by $g(x, y, z, 0) = h(x, y, z)^n$. So

$$\begin{aligned} g_x &= nh^{n-1}h_x + wR_x, \\ g_y &= nh^{n-1}h_y + wR_y, \\ g_z &= nh^{n-1}h_z + wR_z, \\ g_w &= R + wR_w. \end{aligned}$$

Observe that R is not a constant, since g is homogeneous of degree greater than 1. Any point satisfying $h = w = R = 0$ is a singularity of X, contradicting its smoothness. Note that $\mathrm{char}(\mathbb{F}_q)$ does not divide n, since it does not divide d.

Step 3. *If Y is an irreducible surface in $\mathbb{P}^3$ of degree $m < d$ then $X \cap Y$ is irreducible.*

Proof. Suppose $X \cap Y$ is reducible, so let $X \cap Y = C_1 \cup C_2$. Then, by Steps 1 and 2 above, C_i is linearly equivalent to $a_i C_0$ with $a_1 + a_2 = m$. Let the plane which defines C_0 be the plane at infinity, and work in the affine space. We have that there exist polynomials f_1 and f_2 in $\overline{\mathbb{F}}_q[x, y, z]$ such that

$$\begin{aligned} (f_1) &= C_1 - a_1 C_0, \\ (f_2) &= C_2 - a_2 C_0 \end{aligned}$$

and

$$(f_1 f_2) = C_1 + C_2 - mC_0.$$

On the other hand,

$$(f) = C_1 + C_2 - mC_0,$$

where $f = 0$ is the equation for Y, so

$$\left(\frac{f_1 f_2}{f}\right) = (0)$$

which implies that $\exists \lambda \in \overline{\mathbb{F}}_q$ such that $f_1 f_2 = \lambda f$ as functions on X, i.e., $g|(f_1 f_2 - \lambda f)$. But $\deg(g) = d$, and $\deg(f_1 f_2 - \lambda f) \leqslant m < d$, so $f_1 f_2 = \lambda f$ as polynomials, and f factors so Y is reducible. □

Note. Observe that Lemma 2.1 does not work if we drop the condition $m < d$. To see this, consider the following example: Let X be given by $\{g = 0\}$. Start with f_1 and f_2 such that $\deg(f_1) + \deg(f_2) = d$. So $X \cap \{f_1 f_2 = 0\}$ is reducible (call Y_λ the surface given by $\{f_1 f_2 = \lambda\}$). Then Y_λ: $f_1 f_2 + \lambda g$ is a pencil of surfaces with an irreducible member $(X, \lambda = \infty)$ so a generic member is irreducible but $X \cap Y_\lambda = X \cap Y_0$ is reducible.

Back to the code, remember that we need to find a cubic surface $S \subset \mathbb{P}^3$ defined over $\mathbb{F}_q$ containing $q^2 + 2q + 1$ points and having Néron–Severi group of rank 1. If we can manage to find such a surface with the additional condition that there exists a plane that does not intersect it on rational points, we can build a code of length $q^2 + 2q + 1$ by making the plane that does not intersect the surface the plane at infinity. Using random search, we were able to find surfaces in $\mathbb{P}^3$ over $\mathbb{F}_7$ satisfying these requirements. So let us estimate the parameters of such a code in $\mathbb{F}_7$. First, since $q = 7$, we have a surface S with 64 points, which gives us a code of length 64. Using sections of degree at most 2, we have that the dimension of the code is at most 10 (and since S has enough points, we will see that the dimension is exactly 10). Take the linear space of sections to be generated by

$$\{x^2, xy, xz, x, y^2, yz, y, z^2, z, 1\}.$$

Taking a surface $Q \subseteq \mathbb{P}^3$ of degree 2, we see that the intersection $S \cap Q$ is either an irreducible curve or two plane cubics (note that only these are possible because of Lemma 2.1). Let us estimate the maximum number of points on the intersection.

Irreducible case, smooth. Using the adjunction formula, we see that such a curve has genus $g \leqslant 4$. If $g = 4$, we can use the Stöhr–Voloch bound [7] for the number of points, since it admits a classical system (F.K. Schmidt shows in [6] that for curves of genus 4, non-classical system is possible only in characteristics 2 and 5). For a curve $C \in \mathbb{P}^n(\mathbb{F}_q)$ of degree d and genus g, we have that the number of points N is bounded by

$$N \leqslant \frac{1}{n}\big(n(n-1)(g-1) + d(q+n)\big)$$

which in our case $(n = 3, q = 7, g = 4, d = 6)$ gives us $N \leqslant 26$. Observe that this is better than Serre's improvement to Weil's bound $N \leqslant q + 1 + g[2\sqrt{q}\,] = 28$. If $g < 4$ we can use Weil's bound, and have $N \leqslant q + 1 + g[2\sqrt{q}\,] \leqslant 23$.

Irreducible case, singular. To estimate the number of points we use a result by Aubry and Perret (Corollary 2.4 on [1]) which generalizes Weil theorem for singular curves: if C is a curve defined over $\mathbb{F}_q$ with arithmetic genus p_a, the number of rational points of C satisfies

$$\left|\#C(\mathbb{F}_q) - (q+1)\right| \leqslant 2p_a\sqrt{q}.$$

The arithmetic genus of a complete intersection of surfaces of degrees a and b in $\mathbb{P}^3$ is given by

$$p_a(C) = \frac{1}{2}ab(a+b-4) + 1.$$

In our case ($a = 3, b = 2$) the curve has arithmetic genus 4, and at most 29 points.

Reducible case, two plane cubics. For plane curves we use Weil's bound and conclude that each curve has at most 13 points, since $g \leqslant 1$. So the pair has at most 26 rational points.

If $Q \subseteq \mathbb{P}^3$ has degree 1, then Q is a plane, and the intersection is a plane cubic, which has at most 13 points.

We conclude that constructing a code over $\mathbb{F}_7$ using S with 64 points by evaluating functions of degree at most 2, we will obtain an error-correcting code of length 64, dimension at most 10 and minimum distance at least 35. As mentioned before, we have found surfaces satisfying the conditions needed. For ease of notation, we represent a surface as a vector v_f of length 20,

$$v_f = [c_{x^3}, c_{x^2y}, c_{x^2z}, c_{x^2w}, c_{xy^2}, c_{xyz}, c_{xyw}, c_{xz^2}, \ldots, c_{z^2w}, c_{zw^2}, c_{w^3}],$$

where c_m is the coefficient of the monomial m in the polynomial $f \in \mathbb{F}_7[x, y, z, w]$ that defines S. The surface

$$v_f = [5, 6, 1, 1, 0, 5, 0, 3, 6, 3, 5, 1, 0, 5, 0, 5, 0, 0, 2, 4]$$

and the plane

$$6x + 4y + 2z + w = 0$$

give us a [64, 10, 38] code, showing that the bound for the dimension is attained, and the actual minimal distance is larger than the lower bound we have found. This is possible only if the irreducible singular curves (if any) obtained as the intersection of the cubic and quadric surfaces do not attain Aubry and Perret's upper bound for the number of rational points.

Using a similar construction over $\mathbb{F}_9$, we were able to obtain good codes, despite the fact that not all the hypotheses of Lemma 2.1 were satisfied (the characteristic of the field now is 3). Let γ be a generator of the group $\mathbb{F}_9^*$ and using the same notation as above, take the cubic surface represented by

$$v_f = \left[\gamma, \gamma, \gamma^2, \gamma^2, \gamma^5, \gamma^7, \gamma^2, \gamma^2, 1, 0, \gamma, \gamma^5, 2, \gamma^6, \gamma^3, \gamma, 1, \gamma^6, \gamma^2, \gamma^7\right].$$

This surface has 100 rational points and the plane

$$\gamma^6 x + 2y + 2z + w = 0$$

does not intersect the surface over $\mathbb{F}_9$, so we were able to construct a code over $\mathbb{F}_9$ of length 100, dimension 10 and minimal distance 68.

3. Zeta function and Tate's conjecture

Given a variety X of dimension n defined over $\mathbb{F}_q$, we denote the number of points of X whose coordinates lie in $\mathbb{F}_{q^r}$ by N_r. The zeta function of X is defined as

$$Z_X(t) = \exp\left(\sum_{r=1}^{\infty} N_r \frac{t^r}{r}\right). \tag{1}$$

By results of Dwork, Grothendieck and Deligne, we have that $Z_X(t)$ is a rational function that can be written as

$$Z_X(t) = \frac{P_1(t)P_3(t)\dots P_{2n-1}(t)}{P_0(t)P_2(t)\dots P_{2n}(t)}, \tag{2}$$

where $P_0(t) = 1 - t$, $P_{2n}(t) = 1 - q^n t$ and for $1 \leqslant i \leqslant 2n-1$, $P_i(t)$ is a polynomial with integer coefficients, and it can be written as

$$P_i(t) = \prod_{j=1}^{B_i} (1 - \alpha_{ij} t),$$

where the α_{ij} are algebraic integers with $|\alpha_{ij}| = q^{\frac{i}{2}}$, and B_i is the ith Betti number of X. From (1) and (2) it is easy to find that

$$N_r = 1 + q^{nr} + \sum_{i=1}^{2n-1} \left(\sum_{j=1}^{B_i} (-1)^i \alpha_{ij}^r \right). \tag{3}$$

In particular, for surfaces, we have that

$$N_r = 1 + q^{2r} + \sum_{i=1}^{3} \left(\sum_{j=1}^{B_i} (-1)^i \alpha_{ij}^r \right) \tag{4}$$

and this will be important to estimate the rank of the Néron–Severi group of a surface. In [10], Conjecture C, Tate has conjectured that the rank of the Néron–Severi group of a surface S equals the number of α_{2j} in (4) with $\alpha_{2j} = q$. Although equality has not been proved yet, on the same paper he proves that $\operatorname{rk}(NS(S)) \leqslant \#\{\alpha_{2j} \mid \alpha_{2j} = q\}$, as a consequence of the exactness of the sequence 5.10 in [10].

4. Weil restriction of scalars and Néron–Severi rank

Let C be a plane curve defined over $\mathbb{F}_{q^2}$ by $f(x, y) = 0$, but not defined over $\mathbb{F}_q$. Let $g = \text{genus}(C)$. Let $\{1, \alpha\}$ be a basis for $\mathbb{F}_{q^2}$ as a $\mathbb{F}_q$-vector space, with (it will become clear later why we have picked α satisfying this condition)

$$\sigma(\alpha) = \begin{cases} -\alpha & \text{if } 2 \nmid q; \\ -\alpha + 1 & \text{if } 2 \mid q. \end{cases}$$

If x and y are in $\mathbb{F}_{q^2}$, we can write

$$x = x_1 + \alpha x_2,$$
$$y = y_1 + \alpha y_2$$

uniquely with $x_1, x_2, y_1, y_2 \in \mathbb{F}_q$. Moreover, we have that

$$\begin{aligned} f(x, y) &= f(x_1 + \alpha x_2, y_1 + \alpha y_2) \\ &= f_1(x_1, x_2, y_1, y_2) + \alpha f_2(x_1, x_2, y_1, y_2) \end{aligned}$$

with $f_1(x_1, x_2, y_1, y_2)$, $f_2(x_1, x_2, y_1, y_2) \in \mathbb{F}_q[x_1, x_2, y_1, y_2]$. So we can consider the surface S (in 4-dimensional space) defined over $\mathbb{F}_q$ by $f_1(x_1, x_2, y_1, y_2) = f_2(x_1, x_2, y_1, y_2) = 0$. The surface S is denoted by $W_{\mathbb{F}_{q^2}/\mathbb{F}_q}(C)$ and it is called the Weil restriction of scalars of C over $\mathbb{F}_{q^2}$. This is a particular case of the general construction: let k be a finite field and K a Galois extension of k of degree n. Let C be a curve defined over K but not over k. The Weil restriction of scalars of C over K (denoted by $W_{K/k}(C)$) is a variety of dimension n defined over k.

Proposition 4.1. *Given C and $S = W_{\mathbb{F}_{q^2}/\mathbb{F}_q}(C)$ as above, we have that*

$$\#S(\mathbb{F}_{q^k}) = \begin{cases} \#C(\mathbb{F}_{q^{2k}}) & \text{if } k \text{ is odd}; \\ (\#C(\mathbb{F}_{q^k}))^2 & \text{if } k \text{ is even.} \end{cases}$$

Proof. The odd case is straightforward. It follows directly from the construction, since we have that C is defined over $\mathbb{F}_{q^{2k}}$, but it is not defined over $\mathbb{F}_{q^k}$ (if it were defined over $\mathbb{F}_{q^k}$, then it would be also on $\mathbb{F}_{q^k} \cap \mathbb{F}_{q^2} = \mathbb{F}_q$, contradicting our original assumption). So we are left to prove the case k even. For that, we are going to show that

$$S \cong C \times C^\sigma$$

over $\mathbb{F}_{q^k}$ with k even. First, observe that k even implies that $\alpha \in \mathbb{F}_{q^k}$. Using the notation as above for f, f^σ, f_1 and f_2 (with the only difference that now we consider f^σ a polynomial on the variables z and w) we have that we need to show

$$\mathbb{F}_{q^k}[x_1, x_2, y_1, y_2]_{/(f_1, f_2)} \cong \left(\mathbb{F}_{q^k}[x, y]_{/(f)}\right) \otimes_{\mathbb{F}_{q^k}} \left(\mathbb{F}_{q^k}[z, w]_{/(f^\sigma)}\right).$$

We have that

$$\left(\mathbb{F}_{q^k}[x,y]_{/(f)}\right)\otimes_{\mathbb{F}_{q^k}}\left(\mathbb{F}_{q^k}[z,w]_{/(f^\sigma)}\right)\cong\mathbb{F}_{q^k}[x,y,z,w]_{/(f,f^\sigma)}$$

and so

$$\mathbb{F}_{q^k}[x_1,x_2,y_1,y_2]_{/(f_1,f_2)}\cong\mathbb{F}_{q^k}[x,y,z,w]_{/(f,f^\sigma)}$$

follows easily from the identifications (and now becomes clear the choice we made for α)

$$\begin{aligned} x &\leftrightarrow x_1+\alpha x_2,\\ y &\leftrightarrow y_1+\alpha y_2,\\ z &\leftrightarrow x_1+\sigma(\alpha)x_2,\\ w &\leftrightarrow y_1+\sigma(\alpha)y_2. \end{aligned}\qquad\square$$

With the result of Proposition 4.1 and using Tate's conjecture, we are now able to estimate the rank of the Néron–Severi group of a surface S constructed as above. In the case k odd, we have that

$$\#S(\mathbb{F}_{q^k})=\#C(\mathbb{F}_{q^{2k}})=1+q^{2k}-\sum_{j=1}^{2g}\alpha_j^{2k},$$

where the last equality follows from (3) with $n=1$, and in this case, $B_1=2g$. The result above could lead us to think that $\operatorname{rk}(NS(S))\leqslant 2g$. But we have to consider that an eigenvalue and its negative might occur simultaneously, so cancellations can be happening there. So let us take a look at the case k even:

$$\begin{aligned} \#S(\mathbb{F}_{q^k}) &= \left(\#C(\mathbb{F}_{q^k})\right)^2\\ &= \left(1+q^k-\sum_{j=1}^{2g}\alpha_j^k\right)^2\\ &= 1+2q^k+q^{2k}-2\left(1+q^k\right)\left(\sum_{j=1}^{2g}\alpha_j^k\right)+\left(\sum_{j=1}^{2g}\alpha_j^k\right)^2\\ &= 1+2q^k+q^{2k}-2\sum_{j=1}^{2g}\alpha_j^k-2\sum_{j=1}^{2g}(q\alpha_j)^k+\left(\sum_{j=1}^{2g}\alpha_j^k\right)^2. \end{aligned}$$

Observe that eigenvalues equal to q can only come from the terms $2q^k$ and $(\sum_{j=1}^{2g}\alpha_j^k)^2$, since $|\alpha_j|=q^{1/2}$. Also, note that the α_j occur in pairs, i.e., α_j and $\sigma(\alpha_j)$ are both reciprocal of roots of

the polynomial $P_1(t)$ in the zeta function of C. These facts imply that $(\sum_{j=1}^{2g} \alpha_j^k)^2$ will contribute with, at least $2g$, and at most $4g^2$ eigenvalues equal to q, which gives us the estimate

$$2 + 2g \leqslant \operatorname{rk}\big(NS(S)\big) \leqslant 2 + 4g^2,$$

where the second inequality follows from Tate's result in [10], and the first inequality follows from the fact that Tate's conjecture is true for product of curves, proved by himself in [9, Theorem 4].

5. Some codes

We are able now to construct some surfaces and estimate the rank of its Néron–Severi group. We have shown how the rank depends on the genus of the curve C, so we do not want to work with curves of high genus. The first attempt was to use Weil's descent of elliptic curves. We have found reasonable codes, but nothing very impressive. One can say that this happened because the surfaces did not have many points. Roughly speaking, our codes are good if given the surface and a space of curves on this surface, we can get many points laying "outside" of each of these curves. Again, in general terms, we expect a surface to have the square of number of points that a curve has, so it is reasonable to expect that if we do not have many points on the surface, the difference cannot be big enough to give us a good code. With that in mind, we used hyper elliptic curves instead, and we have found better ones. We have constructed codes over $\mathbb{F}_7$ using sections of degree at most 2, more specifically, we took the 11-dimensional $\mathbb{F}_7$-linear space generated by

$$\{x_1 + x_2, y_1 + y_2, \gamma x_1 + \bar{\gamma} x_2, \gamma y_1 + \bar{\gamma} y_2, x_1 x_2, y_1 y_2,$$
$$\gamma x_1 y_2 + \bar{\gamma} x_2 y_1, x_1 y_1 + x_2 y_2, \gamma x_1 y_1 + \bar{\gamma} x_2 y_2, x_1 y_2 + x_2 y_1\}$$

Table 1
Best codes found over $\mathbb{F}_7$ with $n \leqslant 50$

n	k	d	d_{best}	f
50	11	27	28	$y^2 + 6x^5 + \gamma^{27}x^3 + \gamma^6 x^2 + \gamma^{38}x + \gamma^{42}$
48	11	26	27	$y^2 + 6x^5 + \gamma^{28}x^3 + \gamma^4 x^2 + \gamma^{44}x + \gamma^{26}$
42	11	22	23	$y^2 + 6x^5 + \gamma^{29}x^3 + \gamma^{29}x^2 + \gamma^{19}x + \gamma^{19}$
41	11	21	22	$y^2 + 6x^5 + \gamma^{30}x^3 + \gamma^{33}x^2 + \gamma^7$
40	11	20	21	$y^2 + 6x^5 + \gamma^{27}x^3 + \gamma^{25}x^2 + \gamma^{27}x + \gamma^{43}$
39	11	19	20	$y^2 + 6x^5 + \gamma^{27}x^3 + \gamma^{27}x^2 + \gamma^{26}x + \gamma^{30}$
38	11	19	19	$y^2 + 6x^5 + \gamma^{27}x^3 + \gamma^{28}x^2 + 4x + \gamma^{37}$
37	11	18	19	$y^2 + 6x^5 + \gamma^{27}x^3 + \gamma^{29}x^2 + \gamma^{25}x + \gamma^{26}$
36	11	17	18	$y^2 + 6x^5 + \gamma^{27}x^3 + \gamma^{31}x^2 + \gamma^{25}x + \gamma^{27}$
35	11	17	18	$y^2 + 6x^5 + \gamma^{30}x^3 + \gamma^5 x^2 + \gamma^{28}x + 1$
34	11	16	17	$y^2 + 6x^5 + \gamma^{30}x^3 + \gamma^{41}x^2 + \gamma^2 x + \gamma^{22}$
33	11	15	16	$y^2 + 6x^5 + \gamma^{30}x^3 + 5x^2 + \gamma^{22}x + \gamma^{38}$
31	11	14	15	$y^2 + 6x^5 + \gamma^{30}x^3 + \gamma^{10}x^2 + \gamma^{37}x + \gamma^{19}$
30	11	13	14	$y^2 + 6x^5 + \gamma^{30}x^3 + \gamma^{33}x^2 + \gamma^{36}x + \gamma^{23}$
29	11	12	13	$y^2 + 6x^5 + \gamma^{30}x^3 + \gamma^{33}x^2 + \gamma^{26}x + \gamma^{28}$
28	11	12	13	$y^2 + 6x^5 + \gamma^{29}x^3 + 6x^2 + \gamma^{14}x + \gamma^{14}$

Table 2
Best codes found over $\mathbb{F}_7$ with $n > 50$

n	k	d	$d_{\text{best}}/\mathbb{F}_5$	$d_{\text{best}}/\mathbb{F}_8$	f
71	11	42	41	47	$y^2 + 6x^5 + \gamma^{30}x^3 + \gamma^{28}x^2 + \gamma^{38}x + 3$
70	11	41	40	46	$y^2 + 6x^5 + \gamma^{27}x^3 + \gamma^{29}x^2 + 2x + \gamma^{47}$
69	11	41	39	45	$y^2 + 6x^5 + \gamma^{27}x^3 + \gamma^{31}x^2 + \gamma^{38}x + 6$
68	11	40	39	44	$y^2 + 6x^5 + \gamma^{27}x^3 + \gamma^{25}x^2 + \gamma^{17}x + \gamma^{12}$
67	11	39	38	43	$y^2 + 6x^5 + \gamma^{27}x^3 + 4x^2 + \gamma^{31}x + \gamma^{47}$
65	11	38	37	42	$y^2 + 6x^5 + \gamma^{27}x^3 + \gamma^{26}x^2 + \gamma^{33}x + \gamma^{35}$
64	11	37	36	42	$y^2 + 6x^5 + \gamma^{27}x^3 + \gamma^{31}x^2 + 4x + \gamma^{38}$
62	11	36	35	40	$y^2 + 6x^5 + \gamma^{27}x^3 + \gamma^{26}x^2 + \gamma^{44}x + \gamma^{37}$
59	11	34	33	37	$y^2 + 6x^5 + \gamma^{30}x^3 + \gamma^{42}x^2 + \gamma^{27}x + \gamma^{20}$
58	11	33	32	36	$y^2 + 6x^5 + \gamma^{27}x^3 + \gamma^{34}x^2 + \gamma^{33}x + \gamma^{42}$
57	11	32	31	35	$y^2 + 6x^5 + \gamma^{27}x^3 + \gamma^{25}x^2 + \gamma^{36}x + \gamma^{34}$
56	11	31	30	34	$y^2 + 6x^5 + \gamma^{27}x^3 + \gamma^{25}x^2 + \gamma^{38}x + \gamma^{26}$
54	11	30	29	32	$y^2 + 6x^5 + \gamma^{27}x^3 + \gamma^{27}x^2 + \gamma^{26}x + \gamma^{26}$
53	11	29	28	31	$y^2 + 6x^5 + \gamma^{27}x^3 + \gamma^{29}x^2 + \gamma^{29}x + \gamma^{30}$
52	11	29	27	30	$y^2 + 6x^5 + \gamma^{30}x^3 + \gamma^{42}x^2 + \gamma^{18}x + 1$
51	11	28	27	29	$y^2 + 6x^5 + \gamma^{27}x^3 + \gamma^{29}x^2 + \gamma^{9}x + \gamma^{44}$

(where $\bar{\gamma} = \sigma(\gamma)$, σ the Frobenius automorphism of $\mathbb{F}_{49}$, γ a generator of $\mathbb{F}_{49}^*$), and we have found codes with the parameters displayed on Table 1 (n is the length, k is the dimension, d is the minimal distance, d_{best} is the best minimal distance found so far, considering the bounds on minimal distance on linear codes kept by Andries Brower in [3] and $f(x, y) \in \mathbb{F}_{49}[x, y]$ is the polynomial that defines a hyper elliptic curve that gave such a code).

We have also found some codes of length higher than 50, but since Brower's tables do not have yet d_{best} for linear codes over $\mathbb{F}_7$ with $n \geqslant 51$ we compare the codes we have found with the best existing ones over $\mathbb{F}_5$ and $\mathbb{F}_8$. These are shown on Table 2.

Since it would not be very practical to display here all the equations for the hyper elliptic curves that gave us good codes, we have put only one of each. More curves, and the generating matrices for these codes can be found in my web page at http://www.ma.utexas.edu/users/zarzar.

Acknowledgments

I would like to thank Professor Felipe Voloch for the inspiring and motivating conversations. The computations in this paper were made using MAGMA Computational Algebra System.

References

[1] Yves Aubry, Marc Perret, A Weil theorem for singular curves, in: Arithmetic, Geometry and Coding Theory, Luminy, 1993, de Gruyter, 1996, pp. 1–7.
[2] Arnaud Beauville, Complex Algebraic Surfaces, London Math. Soc. Lecture Note Ser., vol. 68, Cambridge Univ. Press, 1983.
[3] A. Brower, Bounds on the minimum distance of linear codes, http://www.win.tue.nl/~aeb/voorlincod.html.
[4] V.D. Goppa, Codes on algebraic curves, Soviet Math. Dokl. 24 (1) (1981) 170–172.
[5] David Mumford, Lectures on Curves on an Algebraic Surface, Ann. of Math. Stud., vol. 59, Princeton Univ. Press, 1966.
[6] F.K. Schmidt, Zur arithmetischen Theorie der algebraischen Funktionen II. Allgemeine Theorie der Weierstrasspunkte, Math. Z. 45 (1939) 75–96.

[7] Karl-Otto Stöhr, José Felipe Voloch, Weierstrass points and curves over finite fields, Proc. London Math. Soc. (3) 52 (1986) 1–19.
[8] H.P.F. Swinnerton-Dyer, The zeta function of a cubic surface over a finite field, Proc. Cambridge Philos. Soc. 63 (1967) 55–71.
[9] John T. Tate, Endomorphisms of abelian varieties over finite fields, Invent. Math. 2 (1966) 134–144.
[10] John T. Tate, On the conjectures of Birch and Swinnerton-Dyer and a geometric analog, in: Séminaire Bourbaki, vol. 9, Exp. No. 306, Soc. Math. France, Paris, 1995, pp. 415–440.